

Web Tools

neko3

Meet the helpers!



Traceroute

How do I get to
that
destination?



Nmap

Network
mapper.



BurpSuite

Intercepting
proxy.

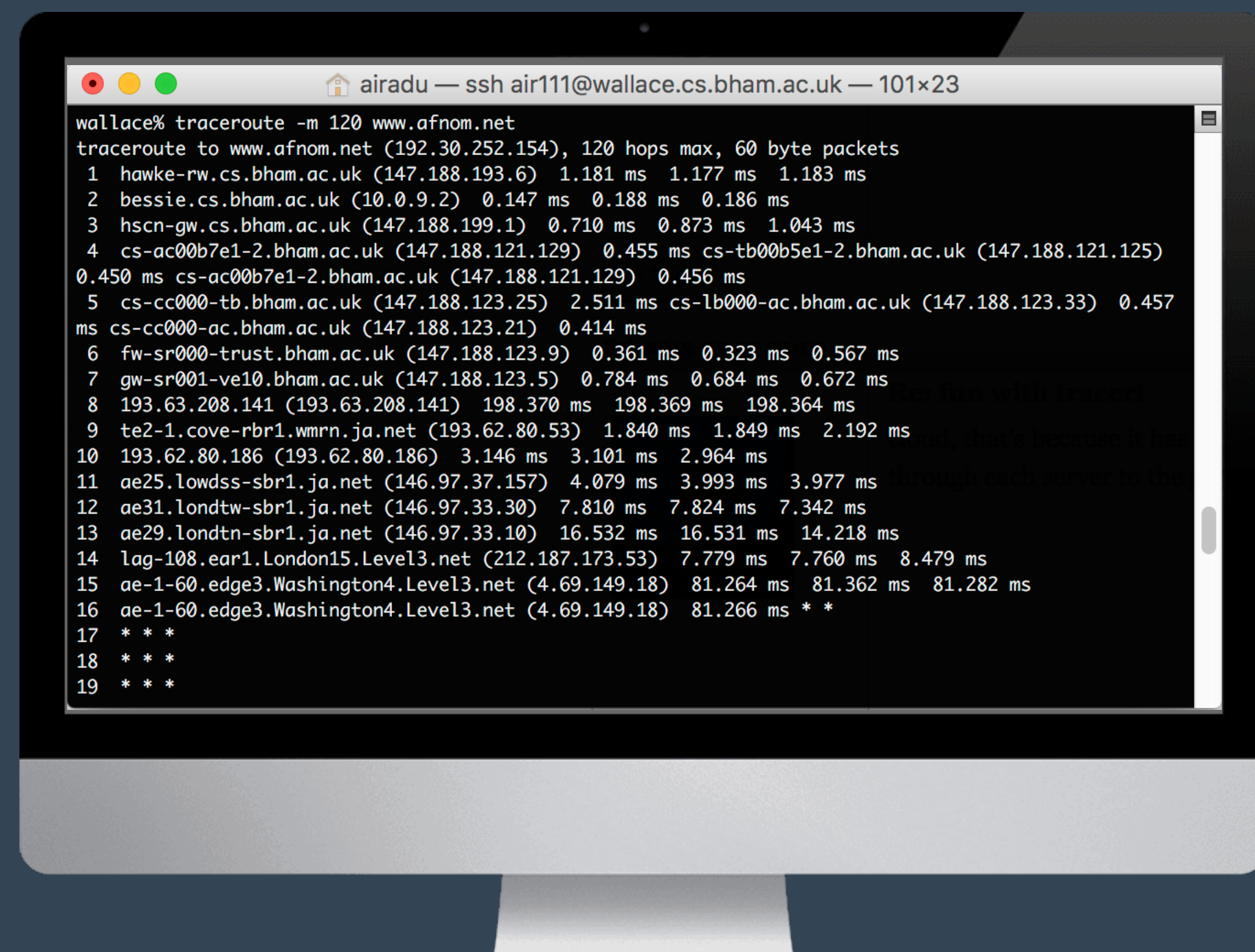


WireShark

Network packet
analyser.

Traceroute

- `traceroute` tracks the route packets taken from an IP network on their way to a given host
- `tracert` on Windows
- `tracpath` on some Linux distros



```
airadu — ssh air111@wallace.cs.bham.ac.uk — 101x23
wallace% traceroute -m 120 www.afnom.net
traceroute to www.afnom.net (192.30.252.154), 120 hops max, 60 byte packets
 1 hawke-rw.cs.bham.ac.uk (147.188.193.6)  1.181 ms  1.177 ms  1.183 ms
 2 bessie.cs.bham.ac.uk (10.0.9.2)  0.147 ms  0.188 ms  0.186 ms
 3 hscn-gw.cs.bham.ac.uk (147.188.199.1)  0.710 ms  0.873 ms  1.043 ms
 4 cs-ac00b7e1-2.bham.ac.uk (147.188.121.129)  0.455 ms  cs-tb00b5e1-2.bham.ac.uk (147.188.121.125)
0.450 ms  cs-ac00b7e1-2.bham.ac.uk (147.188.121.129)  0.456 ms
 5 cs-cc000-tb.bham.ac.uk (147.188.123.25)  2.511 ms  cs-lb000-ac.bham.ac.uk (147.188.123.33)  0.457
ms  cs-cc000-ac.bham.ac.uk (147.188.123.21)  0.414 ms
 6 fw-sr000-trust.bham.ac.uk (147.188.123.9)  0.361 ms  0.323 ms  0.567 ms
 7 gw-sr001-ve10.bham.ac.uk (147.188.123.5)  0.784 ms  0.684 ms  0.672 ms
 8 193.63.208.141 (193.63.208.141)  198.370 ms  198.369 ms  198.364 ms
 9 te2-1.cove-rbr1.wmrn.ja.net (193.62.80.53)  1.840 ms  1.849 ms  2.192 ms
10 193.62.80.186 (193.62.80.186)  3.146 ms  3.101 ms  2.964 ms
11 ae25.lowdss-sbr1.ja.net (146.97.37.157)  4.079 ms  3.993 ms  3.977 ms
12 ae31.londtw-sbr1.ja.net (146.97.33.30)  7.810 ms  7.824 ms  7.342 ms
13 ae29.londtn-sbr1.ja.net (146.97.33.10)  16.532 ms  16.531 ms  14.218 ms
14 lag-108.ear1.London15.Level3.net (212.187.173.53)  7.779 ms  7.760 ms  8.479 ms
15 ae-1-60.edge3.Washington4.Level3.net (4.69.149.18)  81.264 ms  81.362 ms  81.282 ms
16 ae-1-60.edge3.Washington4.Level3.net (4.69.149.18)  81.266 ms  * *
17 * * *
18 * * *
19 * * *
```



When geeks
get bored...

traceroute -m 120 216.81.59.173



```
Tracing route to FIN [216.81.59.173]:
 0  0 ms  0 ms  0 ms  0.0.0.0
 1    76 ms   96 ms   99 ms  192.168.1.254
 2      *      *      *      Request timed out.
 3    18 ms   18 ms   17 ms  195.66.225.189
 4    22 ms   24 ms   24 ms  10gigabitethernet1-1.core1.lon1.he.net
[195.66.224.21]
 5    24 ms   24 ms   24 ms  10gigabitethernet2-4.core1.par2.he.net
[72.52.92.42]
 6    97 ms   97 ms  100 ms  10gigabitethernet7-1.core1.ash1.he.net
[184.105.213.93]
 7   109 ms  109 ms  112 ms  10gigabitethernet1-2.core1.atl1.he.net
[184.105.213.110]
 8   109 ms  108 ms  108 ms  216.66.0.26
 9      *      *      *      Request timed out.
10   149 ms  148 ms  144 ms  Episode.IV [206.214.251.1]
11   146 ms  149 ms  144 ms  A.NEW.HOPE [206.214.251.6]
12   145 ms  149 ms  148 ms  It.is.a.period.of.civil.war [206.214.251.9]
13   147 ms  148 ms  159 ms  Rebel.spaceships [206.214.251.14]
14   147 ms  147 ms  144 ms  striking.from.a.hidden.base [206.214.251.17]
15   144 ms  148 ms  144 ms  have.won.their.first.victory [206.214.251.22]
16   149 ms  147 ms  148 ms  against.theevil.Galactic.Empire
[206.214.251.25]
17   147 ms  157 ms  148 ms  During.the.battle [206.214.251.30]
18   148 ms  152 ms  147 ms  Rebel.spies.managed [206.214.251.33]
19   147 ms  149 ms  149 ms  to.steal.secret.plans [206.214.251.38]
20   146 ms  146 ms  149 ms  to.the.Empires.ultimate.weapon
[206.214.251.41]
21   148 ms  148 ms  149 ms  the.DEATH.STAR [206.214.251.46]
22   150 ms  149 ms  148 ms  an.armored.space.station [206.214.251.49]
23   147 ms  147 ms  148 ms  with.enough.power.to [206.214.251.54]
24   147 ms  149 ms  149 ms  destroy.an.entire.planet [206.214.251.57]
25   145 ms  150 ms  147 ms  Pursued.by.the.Empires [206.214.251.62]
26   146 ms  147 ms  152 ms  sinister.agents [206.214.251.65]
27   150 ms  154 ms  147 ms  Princess.Leia.races.home [206.214.251.70]
28   146 ms  147 ms  148 ms  aboard.her.starship [206.214.251.73]
29   148 ms  151 ms  148 ms  custodian.of.the.stolen.plans
[206.214.251.78]
30   148 ms  147 ms  146 ms  that.can.save.her [206.214.251.81]
31   146 ms  150 ms  147 ms  people.and.restore [206.214.251.86]
32   146 ms  149 ms  149 ms  freedom.to.the.galaxy [206.214.251.89]
33   152 ms  149 ms  148 ms  0-----0 [206.214.251.94]
34   150 ms  147 ms  152 ms  0-----0 [206.214.251.97]
35   148 ms  151 ms  149 ms  0-----0 [206.214.251.102]
36   145 ms  153 ms  146 ms  0-----0 [206.214.251.105]
37   144 ms  148 ms  149 ms  0-----0 [206.214.251.110]
38   145 ms  189 ms  150 ms  0-----0 [206.214.251.113]
39   147 ms  148 ms  149 ms  0-----0 [206.214.251.118]
40   154 ms  146 ms  150 ms  0-----0 [206.214.251.121]
41   148 ms  153 ms  150 ms  0-----0 [206.214.251.126]
42   154 ms  154 ms  149 ms  0-----0 [206.214.251.129]
43   147 ms  147 ms  149 ms  0-----0 [206.214.251.134]
44   150 ms  149 ms  148 ms  0-----0 [206.214.251.137]
45   152 ms  153 ms  156 ms  0-----0 [206.214.251.142]
46   147 ms  152 ms  149 ms  0-----0 [206.214.251.145]
47   172 ms  160 ms  148 ms  0-----0 [206.214.251.150]
48   151 ms  153 ms  154 ms  0---0 [206.214.251.153]
49   149 ms  149 ms  149 ms  0---0 [206.214.251.158]
50   152 ms  149 ms  151 ms  0--0 [206.214.251.161]
51   153 ms  152 ms  151 ms  0-0 [206.214.251.166]
52   150 ms  150 ms  152 ms  00 [206.214.251.169]
53   150 ms  155 ms  149 ms  I [206.214.251.174]
54   152 ms  152 ms  155 ms  By.Ryan.Werber [206.214.251.177]
55   152 ms  153 ms  150 ms  When.CCIEs.Get.Bored [206.214.251.182]
56   151 ms  153 ms  150 ms  read.more.at.beaglenetworks.net
[206.214.251.185]
57   151 ms  151 ms  145 ms  FIN [216.81.59.173]

Trace complete.
```



nmap - network exploration and security auditing tool

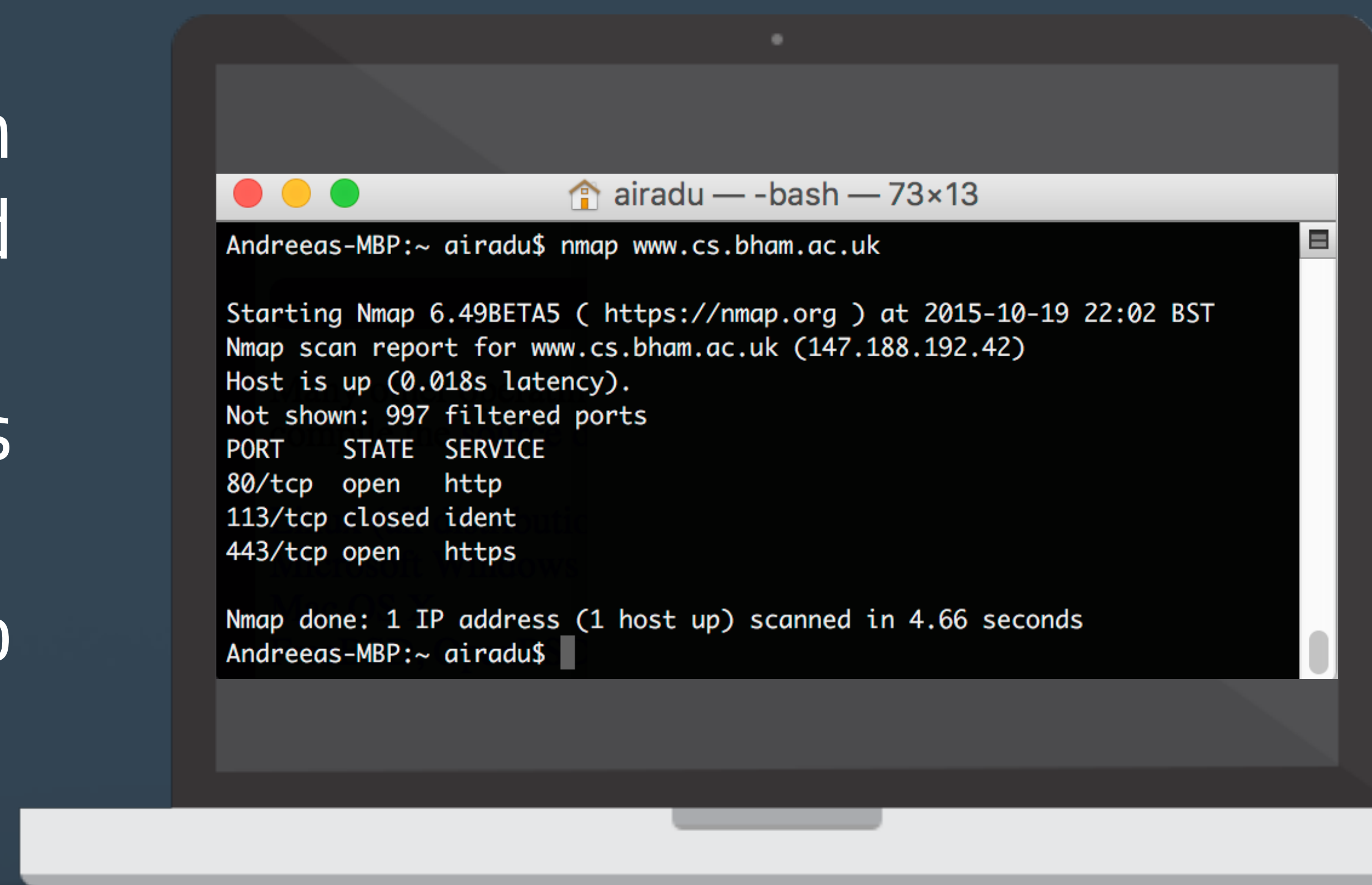
Useful options:

-A: Enable OS detection, version detection, script scanning, and traceroute

-sL: List Scan - simply list targets to scan

-sV: Probe open ports to determine service/version info

<http://nmap.org>



```
airadu — -bash — 73x13
Andreeas-MBP:~ airadu$ nmap www.cs.bham.ac.uk

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-19 22:02 BST
Nmap scan report for www.cs.bham.ac.uk (147.188.192.42)
Host is up (0.018s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 4.66 seconds
Andreeas-MBP:~ airadu$
```



BurpSuite

proxy for intercepting requests between a client (browser) and server (website/service)

The image shows a web browser window displaying a login page for 'Gruyere'. The page has a yellow background with orange circles. It includes links for 'Home', 'Sign in', and 'Sign up'. The main heading is 'Gruyere: Login'. Below this, there are input fields for 'User name' (containing 'monkey') and 'Password' (containing dots), followed by a 'Login' button. A red arrow points from the 'Login' button to the Burp Suite interface.

The Burp Suite interface is overlaid on the right side of the browser window. It shows the 'Proxy' tab selected, with 'Intercept' and 'Intercept is on' buttons. The 'Request to http://google-gruyere.appspot.com:80 [64.233.167.141]' is displayed. The 'Raw' tab is selected, showing the following request details:

```
GET /376675743504/login?uid=monkey&pw=password HTTP/1.1
Host: google-gruyere.appspot.com
Proxy-Connection: keep-alive
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.71 Safari/537.36
DNT: 1
Referer: http://google-gruyere.appspot.com/376675743504/login
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,ro;q=0.6
Cookie: GRUYERE=; GRUYERE_ID=376675743504
```



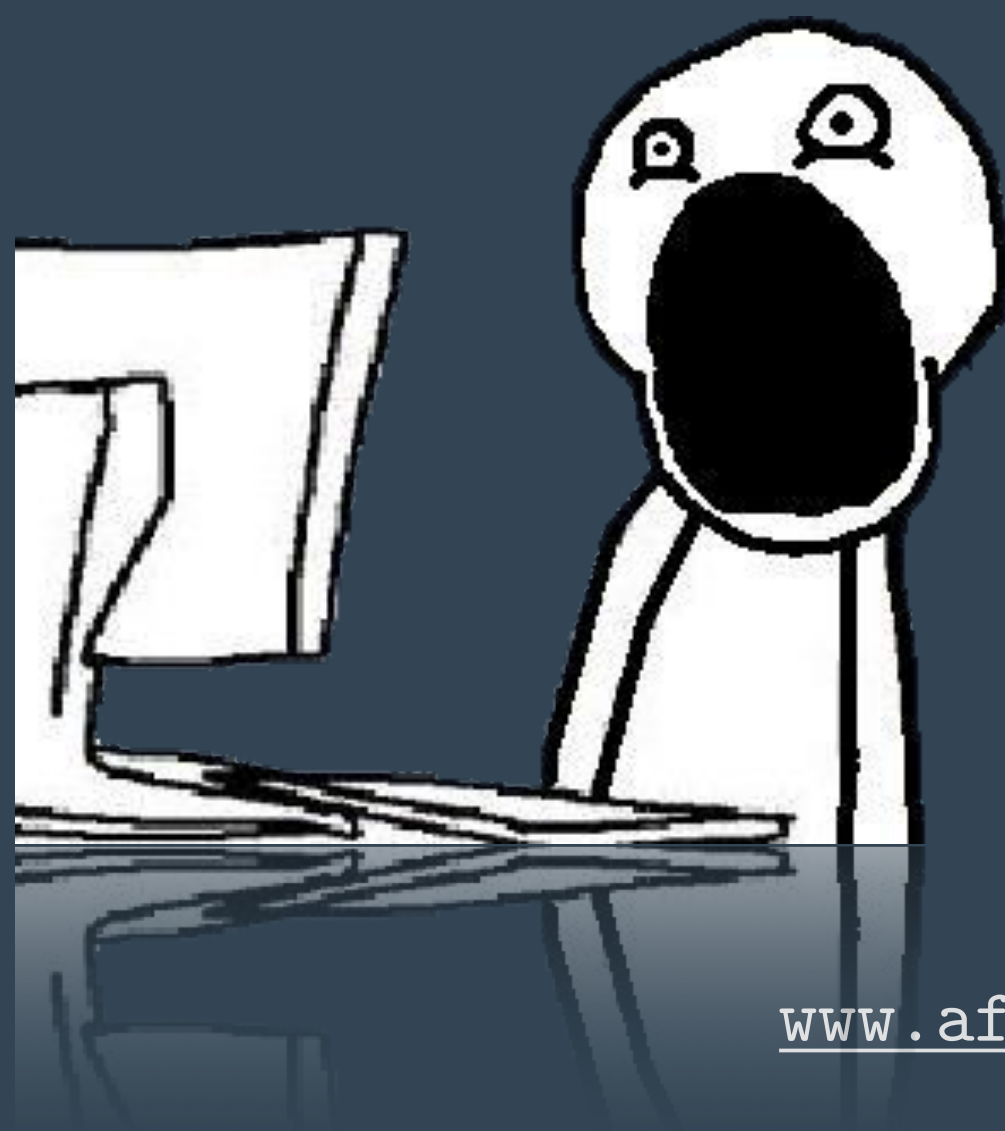
Setting up Burp:

- Set proxy as 127.0.0.1:8080
- Chrome: FoxyProxy from the WebStore
(don't forget to turn it on when you want to intercept)

Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL
✓		Burp		127.0.0.1	8080		5	

- Firefox: Preferences -> Advance -> Network -> Settings

- IE: really?!?!?



www.afnom.net

Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

☒ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080

FTP Proxy: 127.0.0.1 Port: 8080

SOCKS Host: 127.0.0.1 Port: 8080

☐ SOCKS v4 ☒ SOCKS v5 ☐ Remote DNS

No Proxy for:



- Packet analyser
- Capture network traffic
- See protocol communication: SYN – ACK, etc

No.	Time	Source	Destination	Protocol	Length	Info
5963	611.973397000	74.125.136.95	10.8.87.109	TLSv1.2	1470	Server Hello
5964	611.973401000	74.125.136.95	10.8.87.109	TCP	1470	[TCP segment of a reassembled PDU]
5991	611.980014000	10.8.87.109	64.15.119.103	TLSv1.2	301	Client Hello
6062	611.992658000	64.15.119.103	10.8.87.109	TLSv1.2	1470	Server Hello
6063	611.992661000	64.15.119.103	10.8.87.109	TCP	710	[TCP segment of a reassembled PDU]
6065	611.993098000	64.15.119.103	10.8.87.109	TCP	1470	[TCP segment of a reassembled PDU]
6690	767.093498000	10.8.87.109	147.188.127.250	DNS	83	Standard query 0xd596 A safebrowsing.google.com
6692	767.158299000	147.188.127.250	10.8.87.109	DNS	358	Standard query response 0xd596 CNAME safebrowsing.google.com

Frame 5963: 1470 bytes on wire (11760 bits), 1470 bytes captured (11760 bits) on interface 0

Interface id: 0 (en0)

Encapsulation type: Ethernet (1)

Arrival Time: Oct 23, 2015 14:45:49.964221000 BST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1445607949.964221000 seconds

[Time delta from previous captured frame: 0.000400000 seconds]

[Time delta from previous displayed frame: 0.006864000 seconds]

[Time since reference or first frame: 611.973397000 seconds]

0000 3c 15 c2 be 48 ce 00 90 0b 29 02 57 08 00 45 00 <...H...).W..E.

0010 05 b0 96 ba 00 00 28 06 c2 3c 4a 7d 88 5f 0a 08(.<J}._...

0020 57 6d 01 bb c2 73 1c 1f fd ab e9 05 f8 0a 80 10 Wm...s...

0030 01 55 1d 2b 00 00 01 01 08 0a 29 6b a7 33 24 53 .U.+... ..)k.3\$S

0040 49 12 16 03 03 02 c5 02 00 02 c1 03 03 56 2a 3a I.....V*:

0050 0d de a2 bd 2e f3 68 69 46 89 80 de cf 90 54 67hi F....Tg

0060 ab 97 8b a0 86 2a 81 e5 3f 26 04 44 d9 20 57 27*..?&.D. W'

0070 02 1c a5 a9 9d f0 da e1 88 03 64 6a 51 d3 43 69djQ.Ci

0080 40 d5 31 f0 b9 32 e9 ac b8 bb fa 29 11 0f c0 2f @.1..2.. ..).../

0090 00 02 79 ff 01 00 01 00 00 00 00 00 00 12 02 5d ..y.....]

00a0 02 5b 00 77 00 56 14 06 9a 2f d7 c2 ec d3 f5 e1 .[.w.V.. ./.....

00b0 bd 44 b2 3e c7 46 76 b9 bc 99 11 5c c0 ef 94 98 .D.>.Fv. ...\\....

00c0 55 d6 89 d0 dd 00 00 01 50 6c 8f 6c 75 00 00 04 U.....Pl.lu...

00d0 03 00 48 30 46 02 21 00 c1 b4 ca db b3 f0 92 7c ..H0F.!

00e0 39 b6 69 cc 02 67 23 b1 b3 24 89 b7 f3 5a 9f 26 9.i..g#. .\$.Z.&

00f0 58 31 8c 39 18 a0 64 42 02 21 00 ba a5 1a 55 f7 X1.9..dB .!....U.

0100 49 cd 72 da f3 36 d3 cc 84 a5 6a e6 f9 77 2f 3e I.r..6.. ..j..w/>

0110 8b ab d9 7f be 2a 96 b4 f5 61 18 00 76 00 a4 b9*...a.v...

0120 09 90 b4 18 58 14 87 bb 13 a2 cc 67 70 0a 3c 35X... ..gp.<5

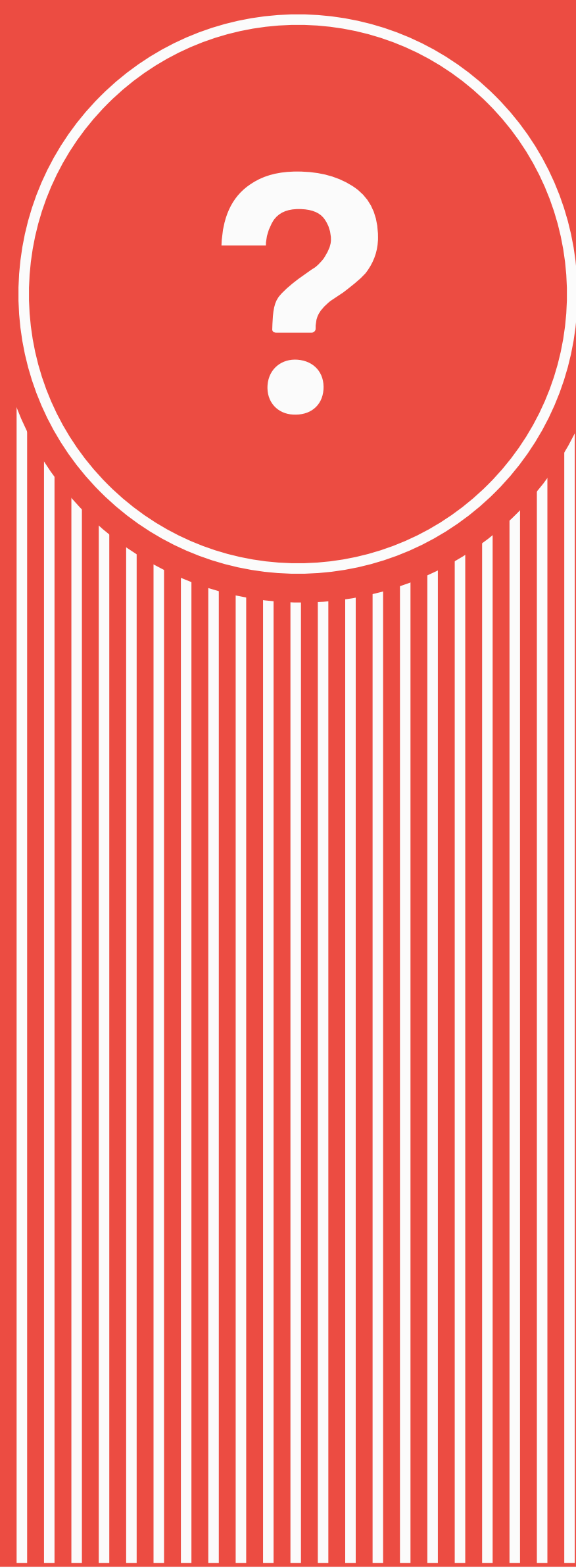
0130 98 04 f9 1b df b8 e3 77 cd 0e c8 0d dc 10 00 00w

Wi-Fi: en0: <live capture in ...> Packets: 7008 · Displayed: 89 (1.3%) Profile: Default

Wi-Fi: en0: <live capture in ...> Packets: 7008 · Displayed: 89 (1.3%) Profile: Default

www.afnom.net





Questions!